IN THE DRAWINGS:

A Replacement Sheet of drawings including revised Figure 4 is attached.

Remarks

Claims 1, 3, 4, 6, 7, 9, 10 and 23-25 are pending in the application.

Claims 1, 3, 4, 6, 7, 9, 10 and 23-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Asokan et al. (US PGPUB No. 20020049601, hereinafter "Asokan") in view of Micali et al. (US Patent No. 4,944,009, hereinafter "Micali").

Each of the various rejections and objections are overcome by amendments that are made to the specification, drawing, and/or claims, as well as, or in the alternative, by various arguments that are presented.

Entry of this Amendment is proper under 37 C.F.R. § 1.116 because the amendment: (a) places the application in condition for allowance for the reasons discussed herein; (b) does not raise any new issue requiring further search and/or consideration since the amendments amplify issues previously discussed throughout prosecution; (c) satisfies a requirement of form asserted in the previous Office Action; (d) does not present any additional claims without canceling a corresponding number of finally rejected claims; or (e) places the application in better form for appeal, should an appeal be necessary. The amendment is necessary and was not earlier presented because it is made in response to arguments raised in the final rejection. Entry of the amendment is thus respectfully requested.

Any amendments to any claim for reasons other than as expressly recited herein as being for the purpose of distinguishing such claim from known prior art are not being made with an intent to change in any way the literal scope of such claims or the range of equivalents for such claims. They are being made simply to present language that is better in conformance with the form requirements of Title 35 of the United States Code or is simply clearer and easier to understand than the originally presented language. Any amendments to any claim expressly made in order to distinguish such claim from known prior art are being made only with an intent to change the literal scope of such claim in the most minimal way, i.e., just to avoid the prior art in a way that leaves the claim novel and not obvious in view of the cited prior art, and no equivalent of any subject matter remaining in the claim is intended to be surrendered.

Also, because a dependent claim inherently includes the recitations of the claim or chain of claims from which it depends, it is submitted that the scope and content of any

dependent claims that have been herein rewritten in independent form is exactly the same as the scope and content of those claims prior to having been rewritten in independent form. That is, although by convention such rewritten claims are labeled herein as having been "amended," it is submitted that only the format, and not the content, of these claims has been changed. This is true whether a dependent claim has been rewritten to expressly include the limitations of those claims on which it formerly depended or whether an independent claim has been rewritten to include the limitations of claims that previously depended from it. Thus, by such rewriting no equivalent of any subject matter of the original dependent claim is intended to be surrendered. If the Examiner is of a different view, he is respectfully requested to so indicate.

Drawings

Applicants have discovered inadvertent typographical error in Figure 4. According to the specification, the "determine hidden value of other party" element should have been designated with reference character "483." (See para. [0047]) Applicants have corrected this error and revised Figure 4. A Replacement Sheet of drawings including revised Figure 4 is submitted herein.

Rejection Under 35 U.S.C. §103(a)

Claims 1, 3, 4, 6, 7, 9, 10 and 23-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Asokan in view of Micali. The rejection is traversed.

Asokan and Micali alone or in combination fail to teach or suggest Applicants' invention of claims 1 and 23, and thus dependent claims 3, 4, 6, 7, 9, 10 and 24-25, as a whole.

The Office Action states that, "There is no disclosure of an iteration of values transferred between users," and "that this appears to be new matter." Accordingly, in the Office Action the term "iteration" is interpreted to be a sequence of values such as generated by Micali. Applicants disagree.

Though Applicants do not use the word "iteration" in describing their invention, what Applicants do describe includes, in fact, iterative processes. Applicants' invention concerns a "fair" exchange of hidden values that obscure digital certificates or passwords

or the like, by a mathematical function such as exclusive-OR or modular multiplication. According to the invention, as disclosed and claimed, sequences of values are revealed and exchanged according to an iterative process wherein each iteration brings the two parties closer to the point at which it is possible for both of them to derive the full hidden information of their respective adverse party.

For example, Figure 4 represents one of the embodiments of the Applicants' invention. As evidenced from Figure 4 and the paragraphs describing Figure 4, [0044-0049], the time line includes at least two sets of entries of identification markers (sequence values) – a "time line for K entries" (block 420) and a "mirror time line" (block 430). These identification markers are transmitted from a first party to the second (other) party. However, they are not transmitted all together at once, but instead, one by one or in groups (Fig. 4, block 485) until all entries of the time line have been transmitted. (See Fig. 4, element 480). Before each next marker or group of markers could be transmitted to the second party, the first party has to receive a comparable entry from the second party. Steps of blocks 485, 460, 470 and 480 – the exchange of the sequence values between the first and the second party – are repeated until all entries of the time line are transmitted. Iteration is a process of repeating, doing something again and again. Accordingly, Applicants disclose the "iteratively exchanging the sequence values" as recited in claim 1, where the number of entries in the time line represents the total number of iterations required to determine the hidden value without forcing such determination.

Further, a modular function of Applicants' invention iteratively produces a plurality of sequence values. As described in the specification, each such sequence value is related to the next previous sequence value. For an example, the sequence from one value to the next one can be produced via squaring or exponentiation by different number of times. (See para. [0032]). Therefore, because the same action has to be repeated over and over, each such action is iteration. Also, paragraph [0037] provides an example of formula [6] that could be used to produce the plurality of the sequence values. Because the formula requires repeating its calculations for different "i" from 0 to K, each of these calculations is iteration. Accordingly, Applicants' amendments of the claims provided with the previous response are fully supported by the specification and do not introduce

new matters.

The Office Action interprets the Asokan reference to disclose the following steps of the Applicants' claim 1:

> "iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values; completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed."

Applicants disagree.

Specifically, the Office Action cites paragraphs [0142] and [0143] of the Asokan reference. These paragraphs have nothing to do with "iteratively exchanging the sequence values." Rather, they disclose that information (set of values) used in encryption process can be requested by one party and stored by another. First, because one party requests but another receives, there is only one party that receives a set of values. This is not exchange, as exchange requires both parties receiving values. Second, paragraphs [0142] or [0143] do not teach or suggest iterative actions. Paragraph [0143] states that, "P can request several coupons at a time." "At a time" means that all requests are sent during one transaction, not iteratively.

Further, though the Asokan reference discloses a method for fair exchange of value items between two parties, the Asokan's invention does not disclose the named above steps. According to the Asokan's invention, there are two major steps in the value exchange proceedings. First, each party sends a permit that allows the receiving party to confirm the value item, but does not allow extracting the item. Second, if both parties accept the permits as correct, thus binding the representation of the expected values, then the parties send the actual value items to each other. (See abstract). Only ones, at the time they exchange/accept permits, does each party verify that the other party is going ahead with the transaction as that party has previously committed. Only ones, the exchange of values takes place. Moreover, the first and second steps involve different actions with different purposes. Therefore, neither of the steps or their combination can be interpreted as iterative exchange.

The Applicants' invention is entirely different. As it was discussed above and as it is disclosed in the specification, during the iterations the first party and second party

successively disclose values that lead up to the end of the sequences. Because the parties know the modular function and the manner of the exchange, during each of the iterations the parties verify that the other party is going ahead as they committed to do, thus doing verification process numerous times. It is possible for each party to determine whether the other party is in conformance with the rules because the successive high or low end values can be tested for exponentiation according to the modular function. When the entire sequence of exchanges is completed, both parties obtain their adverse party's hidden data. However, should either party renege, neither party is at substantial disadvantage because both parties have a comparable computing job to reach the end of the sequence from the information that they have received up to the point that their counterpart reneged. It should be reiterated that, according to Applicants' invention, each party moves towards the hidden value gradually, acquiring the hidden value only through a series of iterations.

Because Asakon does not teach or suggest that the exchange of values should or can be done iteratively, it does not teach or suggest how the number of iteration could be chosen or used, thus it cannot teach or suggest that completing or terminating the exchange of values depends on whether the total number of iterations is completed. In sum, the Asakon reference does not teach at least the named above steps of Applicants' independent claim 1.

The Micali reference does not remedy this gap in Asakon's teaching. The Micali reference simply teaches a random sequence generator that expands an input sequence to an output sequence substantially greater in length than the input sequence via tree structure. It does not involve exchanging values between users, nor does the Office Action provide arguments that it does.

The Office Action states that Micali discloses that difference values between adjacent ones of the sequence values are symmetrically distributed about one of the values of a known order. Applicants disagree. The relevant portions of the Micali reference cited in the Office Action simply teach a random number generator. Micali discloses that Blum integers could be used to generate random numbers. However, using Blum integers in generating random numbers does not necessarily produce symmetrically distributed sequence values. Nowhere in the cited portions does Micali discuss such

symmetry or reasons for seeking such symmetry. If anything, one of ordinary skill in the art might consider symmetry to be an opposite of random. Because Micali teaches generating of random numbers, it does not teach or suggest symmetrical distribution of difference values between adjacent sequence values about one of the values of a known order.

The Office Action also states that the random numbers generated by Micali's invention are the plurality of sequence values of the Applicants' invention because "the random numbers are still in sequence". Applicants disagree.

The Office Action provides a definition of "sequence." According to that definition, the random numbers of Micali have to be "arranged in order and connected by being alike in some way." However, the purpose of generating random numbers is to receive numbers that appear out of order and not connected.

In contrast, the Applicant's plurality of sequence values is more than a succession of random values. The sequence values are values that adhere to a function that enables the receiving party to test (proceeding upwardly and downwardly from the ends of the list toward the center of symmetry or otherwise up to the end of the sequence) that the exchange of values is proceeding according to the agreed function. The Applicant's sequence values demonstrate the continuing participation and good faith of both parties to the transaction. Neither Micali alone, nor in combination with Asokan does Micali teaches or suggest the Applicants' sequence values as recited in independent claim 1.

In sum, the Applicants' invention, claimed as a whole, is not shown by the prior art of record. There is no basis to conclude that the Asokan and Micali disclosures could be combined or applied to produce a method or computing system that meets the subject matter claimed as a whole. Therefore, independent claim 1 is patentable under 35 U.S.C. §103 over Asokan in view of Micali.

Claims 3, 4, 6, 7, 9, and 10 depend directly and indirectly from independent claim 23 and introduce additional limitation thereto. Accordingly, claims 3, 4, 6, 7, 9, and 10 are also patentable over Asokan in view of Micalin under 35 U.S.C. §103.

Further, claim 23 includes relevant limitations to those recited in independent claim 1. Therefore, for at least the same reasons discussed above, claim 23 is patentable under 35 U.S.C. §103 over Asokan in view of Micali. Moreover, the claims 24 and 25

depend directly from claim 23 and introduce additional limitation thereto. Accordingly, claims 24 and 25 are also patentable over Asokan in view of Micalin under 35 U.S.C. §103.

Accordingly, the rejection should be withdrawn.

Conclusion

It is respectfully submitted that the Office Action's rejections have been overcome and that this application is now in condition for allowance. Reconsideration and allowance are, therefore, respectfully solicited.

If, however, the Examiner still believes that there are unresolved issues, the Examiner is invited to call Eamon Wall at (732) 530-9404 so that arrangements may be made to discuss and resolve any such issues.

Respectfully submitted,

Dated: 9/26/07

Eamon J. Wall
Registration No. 39,414
Attorney for Applicants

PATTERSON & SHERIDAN, LLP
595 Shrewsbury Avenue, Suite 100
Shrewsbury, New Jersey 07702
Telephone: 732-530-9404
Facsimile: 732-530-9808

LCNT 125336 (New - 030271)
Serial No: 10/611,711

Garay-10-1 (LCNT/125336)

FIG. 4